有限体上の二重周期系列 : 最大周期平面 (組合せ構造とグラフ理論 II)

AUTHOR(S):

阪田, 省二郎

CITATION:

阪田, 省二郎. 有限体上の二重周期系列 : 最大周期平面 (組合せ構造とグラフ理論 II). 数理解析研究所講究録 1978, 333: 199-220

ISSUE DATE:

1978-09

URL:

http://hdl.handle.net/2433/104173

数理解析研究所講究録
333巻 1978年 199-220

有限体上の二重周期系列（最大周期平面）

相模工大　阪田省二郎

1．はじめに

有限体上の二重周期系列は線形再帰系列（線形フィードバック・シフトレジスタ系列）といわれる周期系列を二次元に拡張したものである。この一般化は必ずしも簡単ではなく、またいくつかの段階が考えられる。二次元化およびより一般的な多次元化が容易でない理由は単純である。それは、一変数多項式環と多変数多項式環の性質の違い、すなわち、前者がユークリッド環であり従って単項イデアル環であるのに対し後者はそうでなく除算が定義されないことによる。[3][9]～[11]

ここでは、二重周期系列の中で特に最大周期平面（M平面）についてのみ論ずる。これは、線形再帰系列の中でも応用上最も重要な最大周期系列（M系列）の二次元化である。M系列は擬似ランダム系列、PN系列ともよばれ、その代数的性質は既に十分に論じられている。M平面は、今後、二次

元情報処理に関して重要になるものと考えられ、平面上の位置の検出や光学系におけるランダムマスクパターン等の応用が図られている。[3][7][4] 我々は以下にM平面の（新しい）定義を与え、さらにM系列からM平面を構成する一般的な方法を示す。その前に、先ず、周知のM系列の主要な性質を簡単に復習しておく。それらが、M平面のどのような性質に拡張されるかを後に見るであろう。簡単のために、2個の元、0と1、からなる体$F \triangleq GF(2)$上の系列に話を限る。

原始多項式（極大多項式）$h(x)=\sum_{i=0}^{m} h_i x^i$, $h_i \in F$, $h_0 = h_m = 1$, に対して、線形再帰関係

$$b_{i+m} = h_{m-1} b_{i+m-1} + \cdots + h_1 b_{i+1} + b_i, \quad i = \cdots, 0, 1, \cdots,$$

を満たす系列 $b=(b_i)$ の全体を $G(h)$ と表す。$G(h)$ の中で零系列（0）でない系列 b を $h(x)$ を特性多項式としてもつM系列という。M系列は以下の性質をもつ。[8]

(1) $b \in G(h) \Rightarrow$ bのシフト $b' = {}_i b$, $b'_j \triangleq b_{i+j}$, $\in G(h)$.

(2) $\#G(h) = 2^m$。2^m 個の各系列は初期条件 $b_0, b_1, \cdots, b_{m-1}$ の相異る 2^m 通りの組によって定まる。さらに $G(h)$ には m 個の（F上）一次独立な系列が存在する。

(3) *window property*：長さ m の窓を一つのM系列の長さ 2^m-1 の部分に沿って滑らせたとき、相異る 2^m-1 通りのすべては0でない内容が丁度一回ずつ現われる。このように

M系列の周期(相異るシフトの総数)は2^m-1である.

(4)一つのM系列の長さ2^m-1の部分は2^{m-1}個の1と$2^{m-1}-1$個の0を含む.

(5) $b, b' \in G(h) \Rightarrow b+b' \in G(h)$.

(6) *shift-and-add property*: $b+_i b \in G(h)$.

(7)M系列bの自己相関々数$\rho(i) \triangleq (1/n)\sum_{j=0}^{n-1}(-1)^{b_j+b_{i+j}}$, $n \triangleq 2^m-1$, は次のように与えられる:

$\rho(0)=1$; $\rho(i)=-1/n$, $1 \leq i \leq 2^m-2$.

(8)M系列において、すべての連のうち半分は長さが1, 1/4は長さが2, 等々である. その各場合において0の連と1の連は同数ある.

(9) bがM系列ならば、bの左右逆転 b', $b'_i \triangleq b_{-i}$, もM系列である. (その特性多項式はhの相反多項式である.)

(10) bがM系列で且つ$(i, 2^m-1)^*=1$ならばbのサンプリング(*decimation*) $b'=b^{(i)}$, $b'_j \triangleq b_{ij}$, もM系列である. (これは一般に別の特性多項式を持つ.)

以上のような性質をもつM系列は原始多項式$h(x)$で定義されるが、一般に$h(x) \mid H(x)$を満たす多項式$H(x)$で定義される系列の全体$G(H)$は、$G(h)$をその部分集合として含

*整数$x, \lambda, \cdots$の最大公約数を$(x, \lambda, \cdots)$で表す.

むことに注意しよう。周期系列bの次元を$b \in G(h)$となる最小次数の多項式$h(x)$の次数mで定義すれば、bがM系列であることは、bの周期が2^m-1に等しいことと等価である。この場合、mはベクトル空間$G(h)$の次元に等しい。原始多項式*は、その根が原始的であるようなF上の既約多項式である。任意のm次既約多項式の根はFの拡大体$GF(2^m)$の原始元θのべきθ^xで表される。ここで、$(x, 2^m-1)=1$はθ^xが再び$GF(2^m)$の原始元であるための必要十分条件であることに注意しておく。

2、二重周期系列

二次元格子$Z^2(=Z\times Z)$から体Fへの写像$u: Z^2 \to F$をFの要素の二重系列或いは平面という。ここで、座標(i,j), $i, j \in Z$, をもつ格子点を$\underline{i}=(i,j)$と書き、その全体を有理整数環ZのべきZ^2と同一視している。$u_{i,j}=u(\underline{i})$として、$u=(u_{i,j})$のように表す。(Z上で一次独立な)$\underline{l}_1, \underline{l}_2 \in Z^2$に対して、$u(\underline{i}+\underline{l}_1)=u(\underline{i}+\underline{l}_2)=u(\underline{i})$, $\underline{i} \in Z^2$, を満たすuを二重周期系列という**。このとき、任意の方向$\underline{l} \in Z^2$に対して、ある正整数kが存在して、$u(\underline{i}+$

---

* これは、代数用語の原始多項式とは異る。

** 二重周期関数との比較。

$k\underline{\ell}) = u(\underline{i}), \underline{i} \in Z^2$, が成立つ。($\because \exists k, k_1, k_2 \in Z$, $k_1\underline{\ell}_1 + k_2\underline{\ell}_2 + k\underline{\ell} = \underline{0}$ と $\underline{\ell}_1, \underline{\ell}_2$ の一次独立性による。) すなわち二重周期系列 u は、任意の方向 $\underline{\ell} \in Z^2$ に対して、周期性をもつ。このような $k\underline{\ell}$ を周期ベクトルという。同方向の周期ベクトルのうち長さ最小のものを基本周期ベクトルという。任意の周期ベクトルは、その方向の基本周期ベクトルの整数倍である。特に、$\underline{i}_x \triangleq (1, 0)$ および $\underline{i}_y \triangleq (0, 1)$ 方向の基本周期ベクトルの大きさを、それぞれ x-偏周期、y-偏周期といい、$per_x(u)$, $per_y(u)$ で表す。(図1)

二重周期系列 u の周期ベクトルを位置ベクトルとしてもつ格子点を u の周期点と呼ぶ。原点から出る一つの基本周期ベクトル $\underline{\ell}_1$ を考える。$\underline{\ell}_1$ を含む直線外でそれに最も近い周期点の一つを $\underline{\ell}_2$ とすると、$\underline{\ell}_1$, $\underline{\ell}_2$ で定まる平行四辺形内には、その周上を含め、その4頂点を除いて周期点は存在しない。このような平行四辺形を u の基本周期平行四辺形といい、$\underline{\ell}_1 \times \underline{\ell}_2$ で表す。この平行四辺形と合同な平行四辺形を隙間なく並べて全平面を敷えば、平行四辺形の網の目が出来上り、その結び目に当る各頂点はいずれも $\underline{\ell} = m\underline{\ell}_1 + n\underline{\ell}_2$, $m, n \in Z$, で表される周期点に対応している。これら以外に周期点は存在しない。u の相異る基本周期平行四辺形 $\underline{\ell}_1 \times \underline{\ell}_2$、$\underline{m}_1 \times \underline{m}_2$ を考えると、整数行列 S, T によって、

$$\begin{pmatrix} \underline{\ell}_1 \\ \underline{\ell}_2 \end{pmatrix} = S \begin{pmatrix} \underline{m}_1 \\ \underline{m}_2 \end{pmatrix}, \quad \begin{pmatrix} \underline{m}_1 \\ \underline{m}_2 \end{pmatrix} = T \begin{pmatrix} \underline{\ell}_1 \\ \underline{\ell}_2 \end{pmatrix}$$

と表される。このことと、$\underline{\ell}_1$, $\underline{\ell}_2$ の一次独立性により、$ST=E$, $\det S \cdot \det T = 1$ が導かれる。これは、S, T が unimodular すなわち $\det S = \det T = \pm 1$ 且つ、$T = S^{-1}$ を意味する。このように、u の任意の基本周期平行四辺形 $\underline{m}_1 \times \underline{m}_2$ は、一つの $\underline{\ell}_1 \times \underline{\ell}_2$ から unimodular 行列 S を用いて、

$$\begin{pmatrix} \underline{m}_1 \\ \underline{m}_2 \end{pmatrix} = S \begin{pmatrix} \underline{\ell}_1 \\ \underline{\ell}_2 \end{pmatrix}$$

と表され、且つそのようなものに限る。（図２）

ある $\underline{\ell} \in Z^2$ に対して、系列 u のシフト $v = {}_{\underline{\ell}}u$ を、$v(\underline{i}) \triangleq u(\underline{i} + \underline{\ell})$, $\underline{i} \in Z^2$ で定義する。二重周期系列 u の相異るシフトの総数は、$\underline{\ell}_1 \times \underline{\ell}_2$ の面積すなわち $\det \begin{pmatrix} \underline{\ell}_1 \\ \underline{\ell}_2 \end{pmatrix}$ の絶対値に等しい。これは、$\underline{\ell}_1 \times \underline{\ell}_2$ 内およびその周上の格子点のうち、周期ベクトルによって重複するものを除いた点の個数である。これを u の周期といい、$per(u)$ で表す。今後これらの $per(u)$ 個の点の集合のことを基本周期平行四辺形 $\underline{\ell}_1 \times \underline{\ell}_2$ と呼ぶことにしよう。一般に、$per(u) \mid per_x(u) \cdot per_y(u)$ である。明らかに、u の任意のシフトは、u と同じ基本周期平行四辺形をもつ。

上で定義した周期 $per(u)$ は次のような性質をもつ。unimodular行列 T と系列 u に対し、系列 $v = \phi_T(u)$ を $v(\underline{i}) \triangleq u(\underline{i}T)$, $\underline{i} \in Z^2$, で定義し、unimodular 変換 T による u の再配列と呼ぶ。これは一対一対応であって、$u = \phi_T^{-1}(v)$ である。$\underline{\ell}$ を周期ベクトルとしてもつ系列 u に対し、$v = \phi_T(u)$ は $\underline{\ell}' = \underline{\ell}T^{-1}$ を周期ベクトルとしてもつ。従って、$\underline{\ell}_1 \times \underline{\ell}_2$ が u の基本周期平行四辺形ならば、$v = \phi_T(u)$ の基本周期平行四辺形 $\underline{m}_1 \times \underline{m}_2$ は、一般に unimodular行列 S に対し、

$$\begin{pmatrix} \underline{m}_1 \\ \underline{m}_2 \end{pmatrix} = S \begin{pmatrix} \underline{\ell}_1 \\ \underline{\ell}_2 \end{pmatrix} T^{-1}$$

で定められる。（図3） このことから特に $per(u) = per(v)$ を得る。この周期のunimodular不変性は、$\underline{k} = \underline{i}S$ に対して $\phi_S(\underline{i}u) = \underline{k}\phi_S(u)$ が成立つことからも導かれる。u の相異るshiftの全体を u のcycleというが、u のcycleは v のcycleに一対一に対応する。無論、一般には $per_x(u) \neq per_x(v)$, $per_y(u) \neq per_y(v)$ である。一次元系列については、再配列に相当する変換は左右逆転だけである。

系列のスカラー倍 $w = c \cdot u$, $c \in F$, 和 $z = u + v$ を通常のように、それぞれ $w(\underline{i}) = c \cdot u(\underline{i})$, $\underline{i} \in Z^2$, と $z(\underline{i}) = u(\underline{i}) + v(\underline{i})$, $i \in Z^2$, で定義する。すべての二重周期系列

の全体Wは、F加群（F上のベクトル空間）になる。例えばuの方向$\underline{\ell} \in Z^2$への周期ベクトルを$m\underline{\ell}$，vの同方向への周期ベクトルを$n\underline{\ell}$とすると、和$z=u+v$は$k\underline{\ell}$，$k=LCM(m,n)$，を周期ベクトルとしてもつ。Wの零元は零系列である。WはF加群であるばかりでなく、F上の二変数多項式環$F[x,y]$の拡大環$\tilde{R} \triangleq \{x^i y^j f(x,y) \mid i,j \in F, f(x,y) \in F[x,y]\}$に対し、$\tilde{R}$加群とみなすことも出来る。そのためには、$\Gamma$を格子点の有限集合として、系列$u$に対する$\tilde{R}$の元、$f(x,y)=\sum_{\Gamma \ni (I,J)} f_{I,J} x^I y^J$の作用$f(x,y): W \to W$を、$v=f(x,y)\cdot u$，$v_{i,j} \triangleq \sum_{\Gamma \ni (I,J)} f_{I,J} u_{i+I,j+J}$，$(i,j) \in Z^2$，で定義すればよい。特に、$x^I \cdot u = {}_{I\underline{i}_x}u$，$y^J \cdot u = {}_{J\underline{i}_y}u$ である。Wの部分$\tilde{R}$加群の中には、ある$f(x,y) \in \tilde{R}$に対して、$f(x,y)\cdot u=(0)$を満す系列uだけからなるものもある。特に、正整数r，sに対し、$per_x(u) \mid r$，$per_y(u) \mid s$，言いかえれば$(x^r+1)\cdot u = (y^s+1)\cdot u=(0)$を満す系列$u$の全体は、$\tilde{R}$加群であり、且つ$r\cdot s$次元の$F$加群である。

二重周期系列uに対し、$f(x,y)\cdot u=(0)$を満す$f(x,y) \in \tilde{R}$の全体が$\tilde{R}$のイデアルをなすことは明らかである。これをuの特性イデアルといい、$\alpha(u)$で表す。$r \triangleq per_x(u)$，$s \triangleq per_y(u)$として、$\alpha(u)$はイデアル(x^r+1, y^s+1)を含む。特に、αの零点集合$V(\alpha)$すなわちαに属するすべての多項

式 $f(x,y)\in F[x,y]$ の共通零点 (α,β) の全体は、$r=r_0\cdot 2^m$, $s=s_0\cdot 2^n$, $(r_0,2)=(s_0,2)=1$, として、1の r_0 乗根の群と1の s_0 乗根の群との直積の部分集合である。

逆に、$\mathfrak{a}$ を $\tilde{R}$ のイデアルとして、すべての $f(x,y)\in\mathfrak{a}$ に対し $f(x,y)\cdot u=(0)$ を満す系列 u の全体 $G(\mathfrak{a})$ は $\tilde{R}$ 加群をなす。$f(x,y)\cdot u=(0)$ を u の成分で書き表した

$$\sum_{\Gamma\ni(I,J)} f_{I,J}\,u_{i+I,j+J}=0,\quad (i,j)\in Z^2,$$

は、所謂、線形再帰関係(定係数斉次線形偏差分方程式)である。$G(\mathfrak{a})\ni u$ を、$\mathfrak{a}$ に対応する線形再帰関係を満す二重線形再帰系列という[11]。正整数 r, s に対し $\mathfrak{a}\supset(x^r+1, y^s+1)$ ならば、$G(\mathfrak{a})$ は W の有限部分 $\tilde{R}$ 加群であり、その F 加群としての次元 $\dim G(\mathfrak{a})$ は $r\cdot s$ より小さい。($\because$ $\mathfrak{a}\supset\mathfrak{b}\Rightarrow G(\mathfrak{a})\subset G(\mathfrak{b})$.) 二重周期系列 u の次元 $\dim(u)$ をその特性イデアル $\mathfrak{a}(u)$ に対し $\dim G(\mathfrak{a}(u))$ で定義する。これは、u を含む極小な $\tilde{R}$ 加群 $G(\mathfrak{a})$ の次元であるといってもよい。$\dim(u)$ は、一次元系列における特性多項式の次数に対応する。

unimodular 行列 $S=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ に対し、$\tilde{R}$ の自己同型写像 $\psi_S:\tilde{R}\to\tilde{R}$ が $\psi_S(f(x,y))=f(x^a y^b, x^c y^d)$, $f(x,y)\in\tilde{R}$, で定義される。$\psi_S^{-1}=\psi_{S^{-1}}$ である。$G(\mathfrak{a})$ のすべての系列 u の S による再配列 $\phi_S(u)$ の全体 $\phi_S(G(\mathfrak{a}))$ は $G(\psi_S^{-1}(\mathfrak{a}))$ に

一致することが証明できる。[12] 特に $\dim(u) = \dim(\phi_S(u))$ である。(∵ϕ_S が線形で一対一であることから明らか。)

3. M平面とその性質

二次元系列で(一次元)M系列に対応するものが多くの著者によって論じられたが、それらは主に window property に焦点を当てたものであった。[1]~[4][8] 特に、その $N_x \times N_y$ 長方形($\triangleq \{(i,j) \mid 0 \leq i < N_x,\ 0 \leq j < N_y\}$)内に沿って $n_x \times n_y$ 長方形の窓を滑らせたとき、相異る $N_x \cdot N_y = 2^{n_x n_y} - 1$ 通りのすべては0でない内容が丁度一回ずつ現れるような二重周期系列 u を最大面積長方形をもつ平面といい、さらに $N_x = per_x(u)$, $N_y = per_y(u)$ のとき u をM平面と定義した。[3][4][6] しかし、この定義には、次元の概念が入っていない。また、一般に $N_x \times N_y$ 長方形には、いくつかの基本周期部分が含まれていることを無視している。

最大面積長方形をもつ二次元系列の例として、$\gamma\beta$-平面が知られている。[4]~[6] やや特殊な形で定義されてはいるが、$\gamma\beta$-平面は既約線形再帰系列の一種である。[13] すなわち、それは R の零次元*素イデアル $\mathfrak{p}$ を特性イデアルとしてもち、W の

*ある正整数 r, s に対し $\mathfrak{a} \supset (x^r+1, y^s+1)$ を満すようなイデアル $\mathfrak{a}$。ベクトル空間の次元とは意味が異る。

（自明な部分加群 $\{(0)\}$ を除いて）極小な部分R加群 $G(\mathfrak{p})$ に属する系列である。ところで素イデアル $\mathfrak{p}$ は、その零点集合 $V(\mathfrak{p})$ によって一意に定められる。また、零次元素イデアル $\mathfrak{p}$ の零点集合は一組の（F上）代数的共役な零点からなるから、一つの零点を指定すれば $\mathfrak{p}$ が定まる。$\gamma\beta$-平面の特性イデアル $\mathfrak{p}$ は、次のような零点 (γ, β) をもつものとして規定される。すなわち、m, n, μ, λ, η を正整数、θ を $GF(2^K)$ の原始元として、

$$\gamma = \theta^{[(2^{m\cdot n}-1)/(2^m-1)]\cdot\mu}, \quad \beta = \theta^{\eta\cdot\lambda}$$

ここで、μ, λ, η は以下の条件を満たすものとする。

(1) $(\eta, 2^{m\cdot n}-1) = 1$,

(2) $\mu\cdot\lambda \mid 2^m - 1$,

(3) $(2^m-1)/\mu \mid 2^k-1 \Rightarrow k \geq m$,

(4) $\left(\lambda, \frac{2^{m\cdot n}-1}{2^m-1}\cdot\mu\right) = 1$.

我々は、前節の考察に基ずいて、改めてM平面を次のように定義しよう。二重周期系列 u に対し $K \triangleq dim(u)$ とおくと、$per(u) \leq 2^K - 1$ が成立つ。最大周期平面（M平面）を $per(u) = 2^K - 1$ を満す系列 u と定義する。このとき、u のすべてのシフトと零系列の全体は $G(\alpha(u))$ に一致し、これ

らはuの基本周期平行四辺形内の各点lに対応する$_l u$の全体によって尽くされる。この性質はM系列の性質(1),(2),(5),(6)に対応する。特にshift-and-add propertyはM平面を特徴づける。すなわち、二重周期系列uがM平面であるための必要十分条件は、uとuの任意のシフトの和が再びuのシフトまたは零系列に一致することである。

M平面の特性イデアルまは零次元素イデアルである。($\because u \in G(\mathfrak{a}), \mathfrak{P} \subsetneqq \mathfrak{a} \subsetneqq \tilde{R} \Rightarrow per(u) \leq 2^{K'}-1, K'=\dim G(\mathfrak{a}) < K$.)従って、M平面は既約線形再帰系列である。まの一つの零点を(α, β)としよう。$K=\min\{K>0 \mid \alpha^{2^K}=\alpha, \beta^{2^K}=\beta\}$だから、$\alpha, \beta \in GF(2^K)$。故に、$GF(2^K)$の原始元$\theta$のべきで$\alpha=\theta^\kappa, \beta=\theta^\lambda$と表される。零系列以外のG(まの系列uは、$u_{i,j}=\sum_{k=0}^{K-1}\theta^{(M+\kappa i+\lambda j)2^k}$, $0 \leq M \leq 2^K-2$で与えられる。これから、$N=2^K-1$として、$per_x(u)=p_x \triangleq \{p_x>0 \mid \kappa \cdot p_x \equiv 0 \bmod N\}=N/(N,\kappa)$, $per_y(u)=p_y \triangleq N/(N,\lambda)$。さらに、$per(u)=p \triangleq N/(N,\kappa,\lambda)$。($\because \mu \triangleq (\kappa,\lambda)$として、$S\cdot\begin{pmatrix}\kappa\\ \lambda\end{pmatrix}=\begin{pmatrix}\mu\\ 0\end{pmatrix}$を満すunimodular行列Sが存在する。素イデアル$\psi_S^{-1}(\mathfrak{P})$は$(\theta^\mu, 1)$を零点としてもつ。$G(\psi_S^{-1}(\mathfrak{P})) \ni u'=\phi_S(u)$はuと同じ周期をもち、$per(u')=per_x(u')=N/(N,\mu)$. Q.E.D.)故に、$per(u)=2^K-1$の条件は、$(2^K-1,\kappa,\lambda)=1$に帰着する。$\gamma\beta$-平面

はこの条件を満し、(我々の定義での)M平面になっていることは明らかである。

αを根としてもつmonicな既約多項式 $f(x)=\sum_{i=0}^{K_1} f_i x^i$, $f_{K_1}=1$, の次数は $K_1 \triangleq \min\{K_1>0 \mid 2^{K_1}\cdot x \equiv x \bmod N\}$ である。また、xを$f(x)=0$を満たすGF(2^{K_1})の元とみて、GF(2^{K_1})上既約なmonic多項式 $h_x(y)=\sum_{j=0}^{K_2'} g_j(x) y^j$, $g_{K_2'}(x)=1$, の次数は $K_2' \triangleq K/K_1$ である。($\because$ $K_2 \triangleq \min\{K_2>0 \mid 2^{K_2}\cdot\lambda \equiv \lambda \bmod N\}$ として、$K=[K_1,K_2]^*$ そして、$K_2'=\min\{K_2'>0 \mid (2^{K_1})^{K_2'}\cdot\lambda\equiv\lambda \bmod N\}$.) これから $h(x,y) \triangleq y^{K_2'}+\sum_{i=0}^{K_1-1}\sum_{j=0}^{K_2'-1} h_{ij}x^i y^j = h_x(y)$, $h_{ij}\in F$, を満すF上既約な多項式が一意に定まり、$\mathcal{F}=(f(x),h(x,y))$である。$u$の満す線形再帰関係は、

$$\begin{cases} u_{i+K_1,j}=\sum_{I=0}^{K_1-1} f_I u_{i+I,j}, \\ u_{i,j+K_2'}=\sum_{I=0}^{K_1-1}\sum_{J=0}^{K_2'-1} h_{IJ} u_{i+I,j+J}, \end{cases} \qquad (i,j)\in Z^2,$$

で与えられる。$\Delta(\mathcal{F}) \triangleq \{(i,j) \mid 0\le i<K_1, 0\le j<K_2'\}$に属するK個の格子点$(i,j)$における$u_{ij}$の値を任意に一組与えれば、上の線形再帰関係を用いて一意にuが定まる。このような2^K通りの相異る初期条件に対応して、$G(\mathcal{F})$のすべての系列が得られる。このようなK個の格子点の集合$\Delta(\mathcal{F})$を$G(\mathcal{F})$の独立点集合という。これは、符号論における情報

*整数$\kappa,\lambda,\cdots$の最小公倍数を$[\kappa,\lambda,\cdots]$で表す。

点集合に相当する。このように、M平面uは、$\Delta(\mathfrak{p})$を窓として、最大面積長方形 $p_x \times p_y'$, $p_y' \triangleq p/p_x$, をもつ。（図6参照） なお、window すなわち独立点集合は上記以外にも選べる。一般にそれがどのように定まるかは、別に論じられている。[11][12]

M系列uのunimodular行列 $S=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$による再配列を $v=\phi_S(u)$とする。vの特性イデアル $\mathfrak{p}' \triangleq \psi_S^{-1}(\mathfrak{p})$はやはり素イデアルで、$(\alpha', \beta')$, $\alpha'=\alpha^a\beta^b$, $\beta'=\alpha^c\beta^d$, はその一つの零点である。前と同様に $\alpha'=\theta^{x'}$, $\beta'=\theta^{\lambda'}$ とおくと、$x' \equiv ax+b\lambda$, $\lambda' \equiv cx+d\lambda \bmod N$である。$S^{-1}$の存在によって、$(N, x, \lambda)=(N, x', \lambda')$を得る。故に、$v$も$u$と同じ周期をもつM平面である。逆に、同じ周期 2^K-1 をもつ任意のM平面はunimodular 変換による再配列およびシフトで互いに移る。（∵同じ周期をもつ系列は、互いに同じ次元をもつ。$(N, x, \lambda)=(N, x', \lambda')$ から、上記の関係を満すSの存在が導かれる。[10]）これらの事実は、M系列の性質（9）,（10）に対応するものである。

4. M平面の構成

周期 $p=2^K-1$ のM系列を垂直方向に繰り返して得られる $per_x(u)=1$, $per_y(u)=2^K-1$ の二重周期系列uは明らか

にM平面である。（図4参照） 前節の終りで述べたことから、このM系列の垂直方向への繰り返しから適当なunimodular行列 $S=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ を用いた再配列およびシフトによって、周期 2^K-1 をもつ任意のM平面を構成することができる。この再配列は、偏周期 $p_x = p/(p,b)$, $p_y = p/(p,a)$ をもつM平面 u の基本周期平行四辺形（または $p_x \times p_y$ 長方形）とM系列の一周期部分との一対一対応を定める。野村ら[4][6] によって示されたγβ-平面とM系列との対応やMacWilliams, Sloane[8] の擬似ランダム平面のM系列からの構成法は、この特殊な場合である。

〔例〕特性多項式 $y^6+y^4+y^3+y+1$ をもつM系列の垂直な繰り返し u は、$\theta^6+\theta+1=0$ を満す $GF(2^6)$ の原始元を θ として、$\mathfrak{p}' \triangleq (x+1, y^6+y^4+y^3+y+1), (1, \theta^{13}) \in V(\mathfrak{p})$ を特性イデアルとしてもつM平面である。（図4） $S=\begin{pmatrix} 11 & 9 \\ -5 & -4 \end{pmatrix}$ によって u を再配列すれば、特性イデアル $\mathfrak{p}=(x^3+x+1, y^2+y+x+1), (\theta^{54}, \theta^{11}) \in V(\mathfrak{p})$ をもち、$per_x(v)=7$, $per_y(v)=63$ のM平面 v（図6）を得る。$\ell_1 \times \ell_2$, $\ell_1=(7,0)$, $\ell_2=(4,9)$, は v の基本周期平行四辺形（図5）、$\Delta=\{(i,j) \mid 1 \le i \le 3, 1 \le j \le 2\}$ は v の独立点集合である。（図6） なお、$\theta'=\theta^{13}$ すなわち $\theta=\theta'^{37}$ とおけば、$\theta^{54}=\theta'^{9}$, $\theta^{11}=\theta'^{59}$ であるから、v は parameters $m=3, n=2,$

$\mu=\lambda=1, \eta=59$ の$\gamma\beta$-平面である。

$S|$による再配列は、$k \equiv 9i-4j \bmod 63$から、k, $0 \leqq k \leqq 63$, と(i, j), $0 \leqq i \leqq 6, 0 \leqq j \leqq 8$, の一対一対応（表1）を定めるが、これはM系列と$\gamma\beta$-平面との対応として既に知られているものと一致する。（野村らは、この対応を二変数多項式と一変数多項式の対応という形で与えている。）M系列からひを構成する方法は、表1に示されたものに限らない。例えば、$S'=\begin{pmatrix}11 & 9\\ 5 & 4\end{pmatrix}$として、$\mathfrak{P}''=\psi_{S'}^{-1}(\mathfrak{P})=(x+1, y^6+y^5+1), (1, \theta^{62}) \in V(\mathfrak{P}'')$, であるから、$k' \equiv 9i-11j$, $0 \leqq i \leqq 6, 0 \leqq j \leqq 8$, はひと y^6+y^5+1 を特性多項式としてもつM系列の対応を定める（表2）。

一般に、同一のM平面の相異る構成法は元のM系列の decimations に対応している。なお、M平面は、その $p_x \times p_y'$ 長方形部分でなく、基本周期平行四辺形によって定まることに注意しよう。

以上のような対応によって、M系列のいくつかの性質がM平面に移される。例えば、M平面の $p_x \times p_y'$ 長方形Γは $2^{K-1}-1$ 個の0と 2^{K-1} 個の1を含む。また、自己相関々数を $\rho(\underline{i}) \triangleq (1/N)\sum_{\underline{j} \in \Gamma}(-1)^{u(\underline{i})+u(\underline{i}+\underline{j})}$ で定義すれば、$\underline{l}_1 \times \underline{l}_2$ を基本周期平行四辺形として、次式が成立つ。

$$\rho(\underline{i}) = \begin{cases} -1/N, & \underline{i} \neq m\underline{l}_1 + n\underline{l}_2 \\ 1, & \underline{i} = m\underline{l}_1 + n\underline{l}_2 \end{cases}, (m,n) \in Z^2.$$

正則な整数行列Aに対し、系列$v = \phi_A(u)$を$v(\underline{i}) \triangleq u(\underline{i}A)$, $\underline{i} \in Z^2$, で定義できる。これはdecimationを二次元へ拡張したものであり、Aがunimodularならば、今まで論じてきた再配列である。このようなA-decimationによるM平面の対応を一般的に論ずることもできる[12][13]が、ここでは省略する。

5. むすび

$\gamma\beta$-平面以外に最大面積長方形をもつ平面が存在するかどうかという問題が以前提起されていた[6]が、これを$\gamma\beta$平面以外に(我々の定義での)M平面が存在するかという問題に置換えてみよう。実は、任意のM平面の特性イデアルは、原始元の適当な変更により$\gamma\beta$-平面の条件(1)～(4)を満すparameters m, n, μ, λ, ηをもつ。このようにしてM平面と$\gamma\beta$-平面との同一性が証明される[10][13]。ここで論じたことが、従来$\gamma\beta$-平面について知られていた事実をより見通しの利く視野の下に再整理しただけでなく、それらの一般的な意味を明らかにしたことを附記しておく。

謝辞

環$\tilde{R}$の自己同型とunimodular変換の応用を御示唆いただいた東京大学工学部伊理正夫教授に深謝いたします。

〈参考文献〉

(1) I. S. Reed, R. M. Stewart: "Note on the existence of perfect maps," IEEE Trans. Inform. Theory, vol. IT-18, p. 10, Jan. 1962.

(2) B. Gordon: "On the existence of perfect maps," IEEE Trans. Inform. Theory, vol. 53, p. 2137, Dec. 1965.

(3) 野村、福田："線形再帰平面と二次元巡回符号，" 電子通信学会論文誌 (A), 54-A, 3, p. 147 (昭46-03).

(4) 野村、宮川、今井、福田："最大面積行列をもつ平面の構成法および諸性質、" 電子通信学会論文誌 (A), 54-A, 5, p. 250 (昭46-05).

(5) 野村、宮川、今井、福田："$\gamma\beta$-平面の諸性質と三次元への拡張，" 電子通信学会論文誌 (A), 54-A, 7, p. 402 (昭46-07).

(6) T. Nomura, H. Miyakawa, H. Imai and A. Fukuda: "A Theory of two-dimensional linear recurring arrays," IEEE Trans., vol. IT-18, no. 6, p. 775 (1972).

(7) M. Harwit: "Spectrometric Imager," Applied Optics, vol. 10, p. 1415 (1971), & vol. 12, p. 285 (1973).

(8) F. J. MacWilliams and N. J. A. Sloane: "Pseudo-random sequences and arrays," Proc. IEEE, vol. 64, no. 12, p. 1715 (1976).

(9) 阪田: "多重線形再帰系列と多重M-系列," 電子通信学会オートマトンと言語研究会資料, AL 76-66 (昭51-12).

(10) 阪田: "多重線形再帰系列とその変換群," 電子通信学会オートマトンと言語研究会資料, AL 76-84 (昭52-03).

(11) 阪田: "二重線形再帰系列とM-系列," 電子通信学会論文誌 (A), 60-A, p. 918 (昭52-10).

(12)* S. Sakata: "General theory of doubly periodic arrays over an arbitrary finite field and its applications,

Part I. Doubly periodic arrays and linear recurring arrays."

(13)* S. Sakata: "General theory of doubly periodic arrays over an arbitrary finite field and its applications, Part II. Irreducible linear recurring arrays and M-arrays."

---

* (12), (13)は, IEEE Trans. Inform. Theoryへ投稿中。

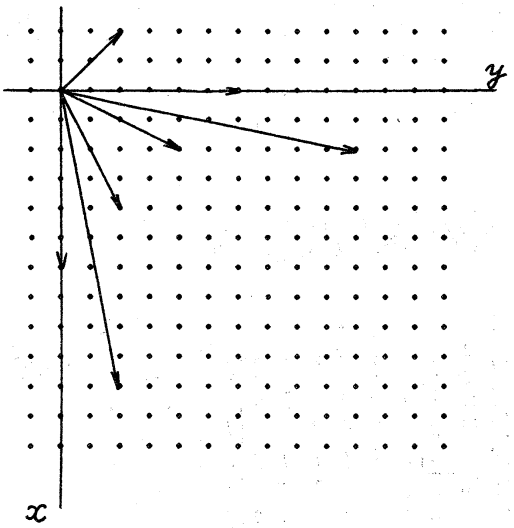

図1. 各方向への
基本周期ベクトル.
(図3のu参照.)

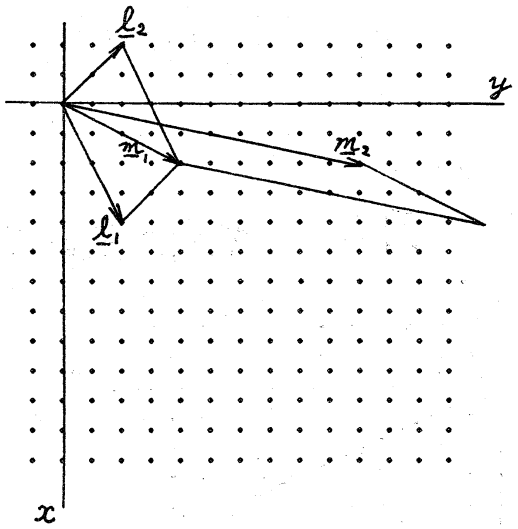

図2. 周期平行四辺形;

$$\begin{pmatrix}\underline{m}_1\\ \underline{m}_2\end{pmatrix}=\begin{pmatrix}1&1\\2&3\end{pmatrix}\begin{pmatrix}\underline{\ell}_1\\ \underline{\ell}_2\end{pmatrix}.$$

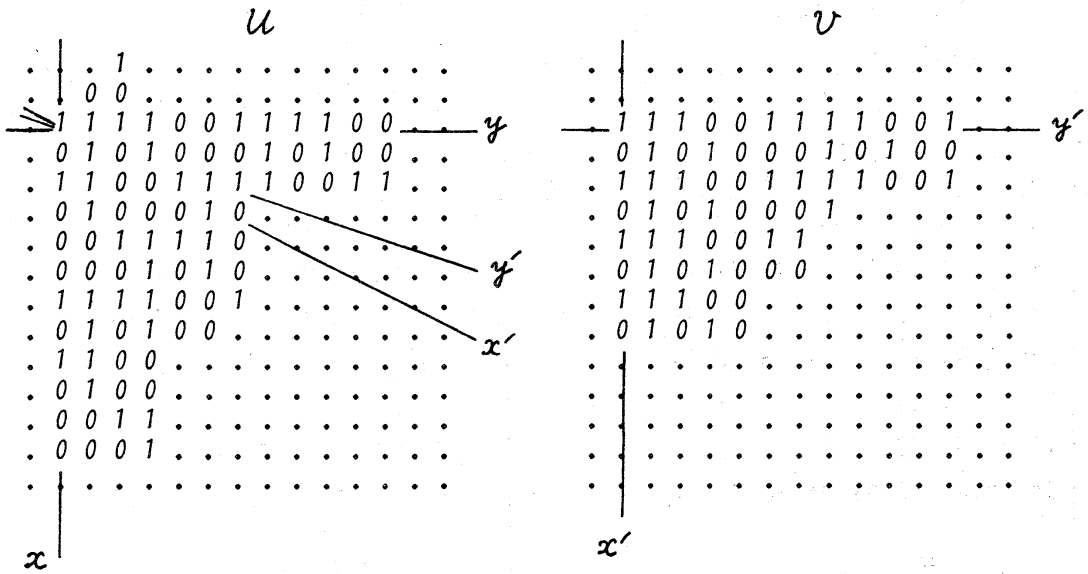

図3. 二重周期系列 u とその再配列 $v=\phi_T(u)$,

$$\begin{pmatrix}2&0\\0&6\end{pmatrix}=S\cdot\begin{pmatrix}4&2\\-2&2\end{pmatrix}\cdot T^{-1};\quad S=\begin{pmatrix}1&1\\4&5\end{pmatrix},\ T=\begin{pmatrix}1&2\\1&3\end{pmatrix}.$$

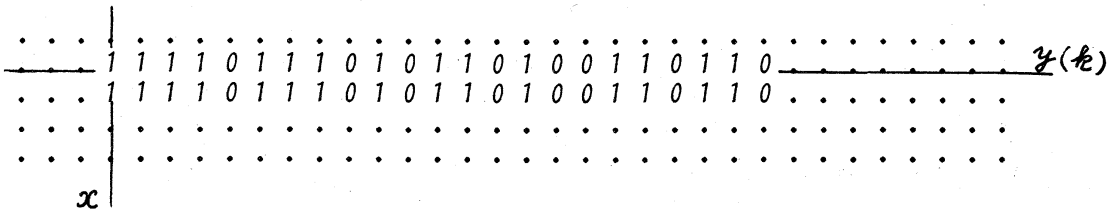

図4. M系列の垂直方向への繰り返し u.

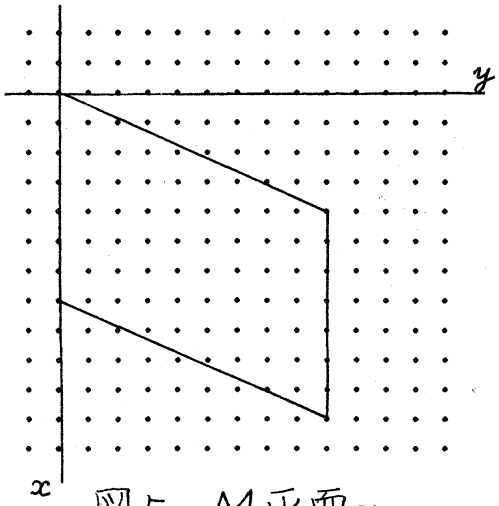

図5. M平面vの周期平行四辺形.

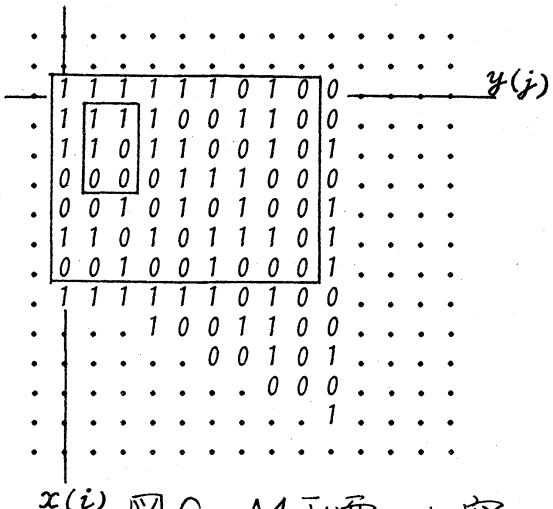

図6. M平面vと窓.
$v=\phi_S(u)$, $S=\begin{pmatrix}11 & 9\\ -5 & -4\end{pmatrix}$.

i \ j	0	1	2	3	4	5	6	7	8
0	0	59	55	51	47	43	39	35	31
1	9	5	1	60	56	52	48	44	40
2	18	14	10	6	2	61	57	53	49
3	27	23	19	15	11	7	3	62	58
4	36	32	28	24	20	16	12	8	4
5	45	41	37	33	29	25	21	17	13
6	54	50	46	42	38	34	30	26	22

表1.(M系列uからの)M平面vの構成法.

i \ j	0	1	2	3	4	5	6	7	8
0	0	52	41	30	19	8	60	49	38
1	9	61	50	39	28	17	6	58	47
2	18	7	59	48	37	26	15	4	56
3	27	16	5	57	46	35	24	13	2
4	36	25	14	3	55	44	33	22	11
5	45	34	23	12	1	53	42	31	20
6	54	43	32	21	10	62	51	40	29

表2. M平面vの(他の)構成法.